Non-COV Mobile Device Security Policy

EFFECTIVE DATE: 11/09/2011, v1

Only the VITAweb Portal has the current version. Verify copy against VITAweb.

PURPOSE: To document the Virginia Information Technologies Agency (VITA) policy on the use of non-Commonwealth of Virginia (COV) owned mobile computing devices to access to COV information technology (IT) resources in conjunction with the COV Information Technology Resource Management (ITRM) IT Security Policy SEC519-00.

SCOPE: All VITA employees, business partners, and those that contract with VITA for services.

ACRONYMS:

BIA:	Business Impact Analysis
CSRM:	Commonwealth Security and Risk Management
COV:	Commonwealth of Virginia
IM:	Incident Management
ISO	(VITA) Information Security Officer
IT:	Information Technology
VITA:	Virginia Information Technologies Agency

DEFINITIONS: See COV ITRM Glossary

STATEMENT OF POLICY/POLICY: This Policy establishes the minimum requirements for the use of non-COV owned and maintained mobile devices to access, process, or store COV data in accordance with IT Security Standard (SEC501). This Policy stipulates the enhanced controls required for mobile devices and does not rescind the obligation to adhere to COV ITRM SEC501-06. At a minimum the selection, implementation and use of mobile devices include the following elements:

Prior to Use

1. The mobile device must be authorized by the Agency Head or his/her designee.
2. The mobile device must be registered with the Agency's Information Security Officer.
3. The mobile device user must read and sign an Agency acceptable use policy for mobile devices. (Such as Attachment A)
4. The device must only be used to access COV data via the COV Messaging Service, a web service accessible from the public Internet, or from a COV internal network in accordance with the COV ITRM IT Standard Use of Non-Commonwealth Computing Devices to Telework SEC 511. This requirement does not apply to the use of Outlook Web Access or restrict the use of the device for personal activities so long

as those activities do not violate any other requirement of any existing COV policy.

5. The mobile device user must agree in writing to allow remote wiping and the erasure of all COV data on the device without warning, if so requested by the Agency Head or the Agency Head designee. The mobile device user must agree in writing to allow remote wiping and the erasure of all data on the device without warning if the COV data cannot be removed without wiping the entire device.
6. The mobile device user must agree to surrender the device to Commonwealth Security for review and forensic imaging upon request of the associated Agency Head or the Agency's Information Security Officer.

Configuration Requirements

1. The mobile device must be configured to receive security policy and configuration information from the COV Mobile Policy Servers.
2. The mobile device must be configured to use an encrypted network connection at all times when accessing COV data.
3. The mobile device screen lock must be configured to engage after a maximum of 15 minutes of inactivity.
4. The mobile device must be configured to prohibit the storage of passwords in clear text.
5. The mobile device must be configured to automatically wipe the contents of the mobile device if a maximum of 10 consecutive invalid login attempts occur.

Password Requirements

1. The mobile device must be configured to use a password in accordance with the COV ITRM Information Security Standard.
2. The mobile device password must be changed after a period of 90 days.
3. The mobile device must be configured to not reuse a password prior to 24 password changes.
4. The mobile device must be configured not to cache/store passwords on the device.
5. The mobile device must be configured to suppress the display of passwords on the screen as the password is entered into the device.

Software Requirements

1. The mobile device must use only the boot ROM and operating system as supplied by the device vendor/carrier.
2. The mobile device must be configured to not allow the user to escalate the base privilege level.
3. The mobile device user must not tamper with security controls configured on the device.
4. The mobile device must install all security updates within 30-days of release by the original equipment manufacturer or the authorized device reseller.

Data Storage Requirements

1. The mobile device shall only store sensitive COV data if approved in advanced by the Agency Head or his/her designee.
2. The mobile device must be configured to require all sensitive COV data be encrypted.
3. The mobile device must utilize an industry-standard encryption protocol to store sensitive COV data (128-bit Advanced Encryption Standard at a minimum).
4. The mobile device must be configured to allow a remote wipe of all COV data stored on the device.
5. The mobile device must be configured to store all COV data only on internal memory or non-removable media.

Physical Security Requirements

1. The mobile device must be protected at all times from unauthorized access.
2. If the mobile device is lost or stolen, the incident must be reported to the VITA Customer Care Center and Commonwealth Security and Risk Management Incident Management within 24-hours in accordance with §2.2-603(F) of the Code of Virginia.
3. The lost or stolen mobile device will be wiped using an automated method within 24-hours of the incident.

Acceptance of this Policy

1. The mobile device user must acknowledge acceptance of and continuing compliance with this policy, including the Code of Virginia, §2.2-2827. The mobile device user will further acknowledge that the Non-COV Mobile Device Security policy may change from time to time and agree to abide by current and subsequent revisions of the policy.

2. This acknowledgement will be made by the mobile device user by signing the "Acknowledgement of Acceptable Use of Non-COV Mobile Device Security Policy" (See: Attachment A) prior to their being granted the right to use a non-COV Mobile Device for COV business purposes.

3. Known instances of non-compliance with this policy should be reported to the employee's supervisor/manager and the ISO.

4. Violations of this Policy will be handled in accordance with DHRM's Standards of Conduct Policy 1.60. Disciplinary action will be determined on a case-by-case basis by the Chief Information Officer or designee, in concert with VITA's Human Resources Office, with sanctions up to/or including termination depending on the severity of the offense.

ASSOCIATED POLICY/ PROCEDURE: None

AUTHORITY REFERENCE:

Code of Virginia, §2.2-2005, et seq.
(Powers and duties of the Chief Information Officer "CIO" Virginia Information Technologies Agency; "VITA")
Code of Virginia, §2.2-2827
(Restrictions on state employee access to information infrastructure)
COV Information Security Policy, ITRM Policy SEC519-00
COV Information Security Standard (SEC501)

OTHER REFERENCE:

Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (SEC514)

IT Risk Management Guideline (SEC506)

IT Data Protection Guideline (SEC507)

IT Systems Asset Management Guideline (SEC518)

Commonwealth Policies, Standards, and Guidelines (PSG):
http://vita.virginia.gov/library/default.aspx?id=537#securityPSGs

VITA Internal Policy Website:
https://vashare.virginia.gov/sites/vita/Resources/PP/Pages/Default.aspx

National Institute of Standards and Technology FIPS 140-2
http://csrc.nist.gov/groups/STM/cmvp/standards.html

Version History		
Version	Date	Change Summary
1	11/09/2011	Original document, which aligns VITA with the requirements in the *IT Security Standard* (SEC501-01),

Attachment A: Acknowledgement of Acceptable Use of Non-COV Mobile Device

ATTACHMENT A

VIRGINIA INFORMATION TECHNOLOGIES AGENCY

ACKNOWLEDGEMENT OF ACCEPTABLE USE OF Non-COV Mobile Device SECURITY POLICY

I understand and agree to abide by current and subsequent revisions to the VITA Policy for Non-COV Mobile Device Policy and the Code of Virginia, Section 2.2-2827.

I understand that VITA has the right to monitor any and all aspects of the Non-COV Mobile Device related to Commonwealth of Virginia data and that this information is a matter of public record and subject to inspection by the public and VITA management for all mobile devices used in the interest of the Commonwealth. I further understand that users should have no expectation of privacy regarding any usage as it relates to Commonwealth of Virginia data, even if the usage was for purely personal purposes. By signing this use agreement the signee agrees to allow remote wiping and the erasure of all COV data on the device without warning, if so requested by the Agency Head or the Agency Head designee. Furthermore, the signee agrees to allow remote wiping and the erasure of all data on the mobile device if the COV data cannot be removed from the device without removing all data from the device. The signee also agrees to surrender the device to Commonwealth Security for review and forensic imaging upon request of the associated Agency Head or the Agency's Information Security Officer.

My signature below acknowledges receipt of the Non-COV Mobile Device Security Policy.

Employee/Business Partner Name (Print) _____

Date_____

Employee/Business Partner Signature: _____

Division/Branch: _____